



Power Your Cyber Ecosystem with  
Synqly's AI-Enabled Integration Platform

Synqly Embedded

# Unmatched Control and Compliance for Security Integrations

Enable Secure OEM Cybersecurity Integrations That  
Your Customers Require

## PROBLEM

Between 2014 and 2022, the enterprise security stack expanded by 760%, creating overwhelming tech sprawl and driving a sharp increase in customer demand for streamlined connectivity. Today, 81% of enterprise security teams are asking for integrated security and IT operations solutions, but most still struggle to achieve them, held back by vendor limitations, proprietary barriers, limited resources, and the compliance risks of third-party SaaS platforms.

For vendors, especially those serving regulated industries like finance, healthcare, utilities, and government, control over data, credentials, and integration workflows is paramount. While cloud architectures are an option for many customers, many organizations continue to maintain critical workloads in a private cloud, private data center, or on-premises. Seamless integrations between products in these environments remain a vital priority. However, most integration platforms can't deliver the required level of control and compliance, forcing development of expensive custom integrations or going without integrations and relying on manual processes.

## SOLUTION

Synqly Embedded brings Synqly's integration capabilities directly into your product, without ever sending sensitive data or credentials to a third-party SaaS environment. It's a self-managed, embeddable integration experience that empowers vendors to deliver native integrations, with no external redirects, no third-party data processing, and no heavy lifting from internal engineering teams.

Built for secure and regulated environments with extremely limited or no external connectivity, Synqly Embedded delivers the full power of Synqly's integration platform in a self-contained, locally deployed package. Synqly Embedded customers retain complete control over all integration operations, credential management, and data flows, eliminating third-party risk and simplifying compliance for regulated industries. With support for local credential management, no external data storage, and the most extensive library of security integrations available, Synqly Embedded empowers vendors to confidently serve air gapped, on-premises, and highly secure environments.

## SYNQLY EMBEDDED DELIVERS

- **Total Data Control:** All data processing, credential management, and integration logic remain within your environment.
- **No Third-Party Data Processing:** Customer data and credentials never leave your infrastructure, ensuring compliance with GDPR, HIPAA, and other regulations.
- **Enhanced Compliance:** Simplified compliance audits and data residency requirements by keeping all integration operations local.
- **Security-First Architecture:** Designed specifically for security, IT Ops, and Managed Services vendors, with double encryption for credentials, local key management, and strong access controls.
- **Air Gapped and Offline Ready:** Fully functional without external connectivity, ideal for air gapped or classified networks.
- **Self-Contained Deployment:** Deploy Synqly Embedded alongside your application in restricted or private environments.
- **Simplified Configuration:** Embeddable UI components walk customers through selecting, configuring, and testing integrations.
- **Custom Branding:** White-label the experience to reflect your product and design system.
- **Accelerated Time-to-Market:** Significantly speed up integration, development, and deployment in private data centers and cloud infrastructure.
- **Cost Reduction:** Reduce integration costs by up to 90%.
- **Unified API, Connect Once to Many:** Single integration to connect with all the vendors in a category.
- **Ongoing Metrics and Support:** Insights into usage data, connection failure, incident timing, and cause analysis.
- **Standardization:** Leverage industry standards like OCSF and STIX for improved interoperability.
- **Resource Optimization:** Free up engineering resources to focus on core product development.

## TECHNICAL CAPABILITIES

- **High-Volume Throughput:** Synqly Embedded has been tested to handle sustained loads of 10,000+ requests per second without service degradation, ensuring confidence in performance at scale.
- **No Hidden Bottlenecks:** The service architecture is free of soft caps that could silently limit throughput. Scalability is determined by available resources, not platform constraints.
- **Proactive DDoS Mitigation:** Internal safeguards include a global rate limiter to maintain platform reliability and protect against misuse.
- **Air Gapped Deployment Support:** Run Synqly Embedded in disconnected or highly restricted systems.
- **Unified Data Schema:** Based on OCSF and industry standards for cross-product integration.
- **Adaptive Data Mapping:** Users can define mappings with source paths, destination paths, and data types.
- **Unified Query Language:** Write a single query and Synqly normalizes the query to the underlying language of all products within a given category.
- **Automated Maintenance:** Persistent API monitoring, tracking changes, and releasing updates as needed to maintain integration health.
- **Native Prometheus Support:** Export Prometheus-formatted metrics for real-time observability.
- **Comprehensive Monitoring:** Visibility into usage, performance, and issues for all integrations.
- **Connect UI:** Option drop-in UI elements for self-service creation of integrations.
- **Security First Design:** Double encryption for credentials; no customer data stored by Synqly.
- **Data Transparency:** Built for compliance so that credentials and sensitive data never leave your infrastructure.

## RESOURCE REQUIREMENTS

Synqly Embedded is delivered as a lightweight, containerized service. It is designed for flexible deployment into restricted environments, including air gapped systems. Deployment is typically managed via Helm within a Kubernetes cluster, but may also be adapted for virtual machine (VM) environments based on customer needs.

## PRE-PRODUCTION / TEST ENVIRONMENT SYSTEM GUIDELINES

For evaluation, POCs, or minimal load testing environments:

| Component                | CPU (vCPUs) | Memory (GB) |
|--------------------------|-------------|-------------|
| Embedded                 | 1.0         | 1.5         |
| Management UI            | 0.5         | 1.0         |
| Connect UI               | 0.5         | 1.0         |
| Scaling Room (buffer)    | 1.0         | 0.5         |
| <b>Total Recommended</b> | <b>3.0</b>  | <b>4.0</b>  |

*Note: Resource planning should always include headroom to support unexpected load and vertical scaling in air gapped environments.*

## PRODUCTION ENVIRONMENTS SYSTEM GUIDELINES

For high-throughput or enterprise-scale deployments with sustained traffic (e.g., 600K requests/min):

| Component                                   | CPU (vCPUs) | Memory (GB) |
|---------------------------------------------|-------------|-------------|
| Embedded (based on June 2024 load test)     | 8.0         | 12.0        |
| Management UI + Connect UI                  | 1.0         | 2.0         |
| Embedded Scaling Buffer (post-June updates) | 1.0         | 2.0         |
| <b>Total Recommended</b>                    | <b>10.0</b> | <b>16.0</b> |

*Note: These values are based on sustained performance at 600K simple requests per minute and account for platform evolution since the last load test.*

### Infrastructure Requirements

- **PostgreSQL-Compatible Database (external)**
- **Kubernetes Cluster** (external)
- **Key Management System (KMS):**  
Supported: AEAD, AWS KMS, Azure KMS, GCP KMS, HashiCorp Vault Transit
- **SMTP Server** (Required if using Management UI)

### Ingress & TLS Support

Synqly Embedded supports multiple methods for TLS termination, including:

- **Kubernetes Ingress Controllers** (e.g., NGINX)
- **K8s Ingress Controllers** (e.g. ingress-nginx, aws-load-balancer-controller)
- **Externally Managed Load Balancer**

### Initialization and Deployment

On initial deployment, the Embedded Pod will automatically create a default organization and output the access credentials to Pod logs, with the option to turn off logging. These credentials are used to authenticate with the Synqly API. Deployment is managed via the Synqly Embedded Helm Chart, which provisions all necessary Kubernetes components and configuration files.

## ABOUT

Synqly is the first integration platform purpose-built for security, IT Ops, and Managed Service vendors. Our unified API enables rapid, seamless integrations, without draining engineering resources, reducing development costs and complexity by up to 90%. Synqly sets the new standard for scalable, efficient security integrations.